Cisco Cloud Security for SMB

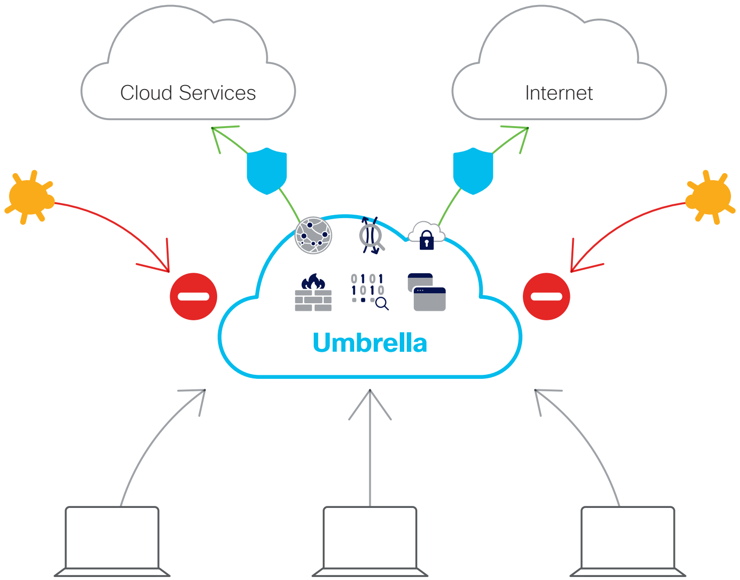
Cisco Umbrella

CISCO DESIGNED

Multiple Security Functions in a Single Cloud Security Service: Cisco Umbrella

Cisco Umbrella secures internet access and controls cloud app usage from your network, branch offices, and roaming users. Unlike disparate security tools, Cisco Umbrella unifies DNS-Layer Security, Secure Web Gateway (SWG), Cloud Access Security Broker (CASB), Cloud-Delivered Firewall (CDFW), Data Loss Prevention (DLP), and Remote Browser Isolation (RBI) functionalities into a single cloud service.

Cisco Umbrella acts as a secure on-ramp to the internet and delivers deep inspection and control to support compliance and provide effective threat protection. Backed by Cisco Talos, one of the largest threat intelligence teams in the world, Cisco Umbrella exposes threats for better investigation and response. By delivering all this from the cloud, Umbrella offers visibility and enforcement to protect users anywhere.



Highlights

- **DNS-Layer Security**
  By enforcing security at the DNS and IP layers, Cisco Umbrella blocks requests to malicious and unwanted destinations before a connection is even established – stopping threats over any port or protocol before they reach your network or endpoints.
- **Secure Web Gateway (SWG)**
  Cisco Umbrella includes a cloud-based full proxy that can log and inspect all of your web traffic for greater transparency, control, and protection. IPsec tunnels, PAC files, and proxy chaining can be used to forward traffic for full visibility, URL and application-level controls, and advanced threat protection.
- **Cloud Access Security Broker (CASB)**
  Cisco Umbrella helps expose shadow IT by detecting and reporting on cloud applications in use across your environment. Insights can help manage cloud adoption, reduce risk and block the use of offensive or inappropriate cloud applications.
- **Cloud-Delivered Firewall (CDFW)**
  Cisco Umbrella cloud-delivered firewall provides visibility and control for traffic that originated from requests going to the internet, across all ports and protocols.
- **Data Loss Prevention (DLP)** NEW
  Cisco Umbrella data loss prevention analyzes sensitive data in-line to provide visibility and control over sensitive data leaving your organization.
- **Remote Browser Isolation (RBI)** NEW
  By isolating web traffic from the user device and the threat, Cisco Umbrella remote browser isolation delivers an extra layer of protection to the Umbrella secure web gateway so that users can safely access risky websites.

Cisco Cloud Security for SMB

Cisco Umbrella

CISCO DESIGNED

Cisco Umbrella Package Comparison

Security & Controls			DNS Security Essentials	DNS Security Advantage	SIG Essentials	SIG Advantage NEW
DNS-Layer Security	Block domains for malware, phishing, botnet, and other high risk		✓	✓	✓	✓
	Block domains from Cisco SecureX, direct integrations (Splunk, Anomali, & others), and custom lists using enforcement API		✓	✓	✓	✓
	Block direct-to-IP traffic for C2 callbacks that bypass DNS[*1]			✓	✓	✓
Secure Web Gateway (SWG)	Proxy web traffic for inspection [Decrypt and inspect SSL (HTTPS) traffic]			Risky domains only	✓	✓
	Enable web filtering	Of domains	✓	✓	✓	✓
		Of URLs			✓	✓
	Create custom block/allow lists	Of domains	✓	✓	✓	✓
		Of URLs			✓	✓
	Block URLs based on Cisco Talos and other feeds; block files based on AV Engine and malware defense			Risky domains only	✓	✓
	Use Secure Malware Analytics (sandbox) on suspicious files				500 samples/day	Unlimited samples
	Use retrospective security to identify previously-benign files that became malicious				✓	✓
Cloud Access Security Broker	Discover and block shadow IT with App Discovery report	Of domains	✓	✓	✓	✓
		Of URLs			✓	✓
	Create policies with more granular controls (block uploads, attachments, and posts) for select apps				✓	✓
	Scan and remove malware from cloud-based file storage apps NEW				2 applications	All supported applications
Cloud-Delivered Firewall (CDFW)	Create layer 3/layer 4 policies to block specific IPs, ports, and protocols				✓	✓
	Deepen protection for outbound traffic using application layer 7 policies with intrusion prevention system (IPS) NEW				Add-on	✓
	Use IPsec tunnel termination				✓	✓
Data Loss Prevention (DLP)	Enable inline inspection of web and cloud app traffic for sensitive data NEW				Add-on	✓
Remote Browser Isolation (RBI)	Provide safe access to risky sites, web apps and all web destinations NEW				Add-on	Add-on
XDR and Threat Intelligence	Integrate with SecureX to aggregate activity across Cisco products	Reporting & enforcement APIs	✓	✓	✓	✓
		All APIs		✓	✓	✓
	Access Umbrella's deep domain, IP, and ASN data for rapid investigations			✓	✓	✓

[*1] Endpoint footprint (Umbrella Roaming Client, Umbrella Chromebook Client, or Umbrella Roaming Security Module for AnyConnect) is required.

Cisco Umbrella Licenses NEW

Product SKU[*1]	Description
UMB-DNS-ESS-K9	Umbrella DNS Security Essentials per User License (1 ~ Users)
UMB-DNS-ADV-K9	Umbrella DNS Security Advantage per User License (1 ~ Users)
UMB-SIG-ESS-K9	Umbrella Secure Internet Gateway Essentials per User License (1 ~ Users)
UMB-SIG-ADV-K9	Umbrella Secure Internet Gateway Advantage per User License (1 ~ Users)
UMB-WLAN	Umbrella WLAN per Access Point License (5 ~ APs)

*1 UMB-SEC-SUB is required in CCW. See Ordering Guide for details.

Ordering and Licensing Guide

Cisco Umbrella is licensed on a subscription basis. Each customer has only one subscription, though each subscription may comprise multiple products (Umbrella, Investigate, and others). Subscriptions are available for standard term lengths of 12, 36, and 60 months. Following the completion of the term, the subscription will be renewed automatically for an additional 12-month term unless the renewal is canceled or auto-renewal was deselected at the time of the initial order. Subscriptions can be changed mid-term or manually renewed.

Seat-based Licensing

Cisco Umbrella DNS Security and Secure Internet Gateway are licensed per seat. A seat is defined as an Internet-connected user who may have access to the service. Seat counts are independent of the number of devices or endpoints protected.
Minimum one seat is required to purchase.

Cisco Umbrella Add-on Licenses NEW

Product SKU[*1]	Description
UMB-L7-CDFW	Umbrella L7 Cloud Firewall License[*2]
UMB-DLP	Umbrella Data Loss Prevention License[*2]
UMB-RBI-RISKY	Umbrella Remote Browser Isolation (Isolate Risky) License
UMB-RBI-WEBAPP	Umbrella Remote Browser Isolation (Isolate Web Apps) License
UMB-RBI-ALL	Umbrella Remote Browser Isolation (Isolate Any) License

*1 UMB-SEC-SUB is required in CCW. See Ordering Guide for details.
*2 Add-on for Umbrella SIG Essentials.

Cisco Umbrella Roaming License

Product SKU[*1]	Description
UMB-ROAM	Umbrella Roaming per User License

*1 UMBRELLA-SUB is required in CCW.

Cisco Umbrella Branch Licenses

Product SKU[*1]	Description
UMB-BRAN-RV	Umbrella Branch License for Cisco RV 340 Series
UMB-BRAN-1100	Umbrella Branch License for Cisco ISR 1100 Series
UMB-BRAN-4221	Umbrella Branch License for Cisco ISR 4221
UMB-BRAN-4321	Umbrella Branch License for Cisco ISR 4321
UMB-BRAN-4331	Umbrella Branch License for Cisco ISR 4331
UMB-BRAN-4351	Umbrella Branch License for Cisco ISR 4351
UMB-BRAN-4431	Umbrella Branch License for Cisco ISR 4431
UMB-BRAN-4451	Umbrella Branch License for Cisco ISR 4451

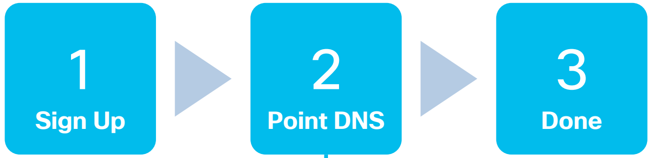
*1 UMBRELLA-SUB is required in CCW.

Enterprise-wide Deployment in Minutes

Cisco Umbrella is the fastest and easiest way to protect all of your users in minutes. Because it is delivered from the cloud, there is no hardware to install or software to manually update. You can provision all on-network devices —including BYOD and IoT— in minutes and use your existing Cisco footprint to quickly provision thousands of network egresses and roaming laptops.

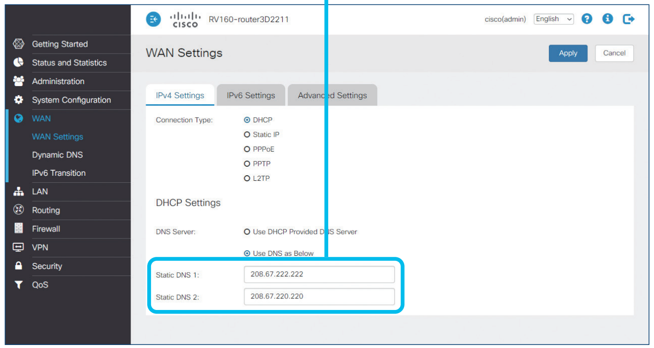
Additionally, with the Cisco Security Connector app, you can use the Umbrella extension to protect supervised iOS 11.3 or higher devices.

How Easy Is It to Deploy Umbrella?


1 Sign Up

2 Point DNS

3 Done



WAN Settings

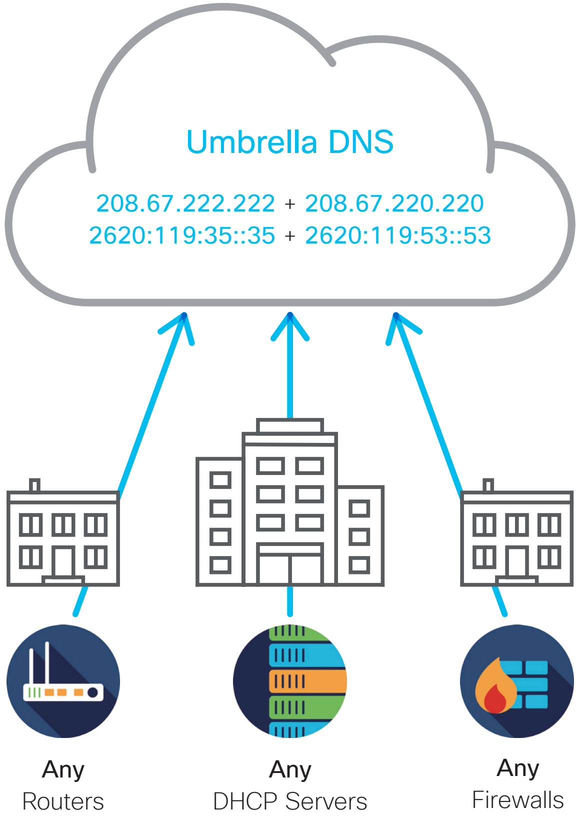
Connection Type: ● DHCP ○ Static IP ○ PPPoE ○ PPTP ○ L2TP

DHCP Settings

DNS Server: ○ Use DHCP Provided DNS Server ● Use DNS as Below

Static DNS 1: 208.67.222.222

Static DNS 2: 208.67.220.220


Umbrella DNS

208.67.222.222 + 208.67.220.220

2620:119:35::35 + 2620:119:53::53

Off-Network Security without VPN

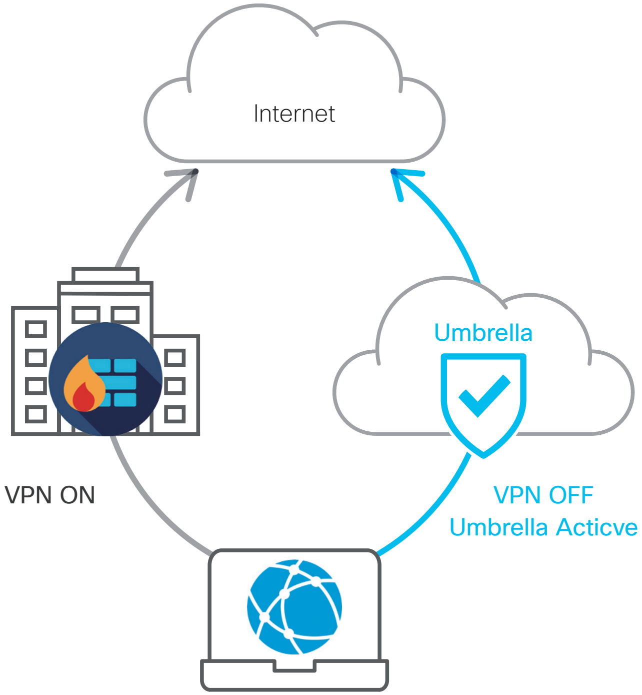
Cisco Umbrella protects employees when they are off the VPN by blocking malicious domain requests and IP responses as DNS queries are resolved. By enforcing security at the DNS-layer, connections are never established and files are never downloaded. This protects against malware, command & control (C2) callbacks, and phishing attacks and helps detect the exfiltration of data over any port.

The Way Your Employees Work Has Changed

82% of your workers admit to not always using the VPN[*1]
Employees are using more cloud apps for work and leveraging their work laptops for personal use—the reality is that not every connection goes through the VPN. Your network extends beyond the perimeter, and your security must too.

49% of your workforce is mobile and under defended[*2]
Zero-day malware spikes at night and on weekends when we're roaming and attackers know we're vulnerable. In fact, 22% of malicious email links are clicked when roaming.[*3] While security may never stop 100% of the threats, it must work 100% of the time.

*1 cs.co/IDG-survey *2 cs.co/sans-survey *3 cs.co/proofpoint-report

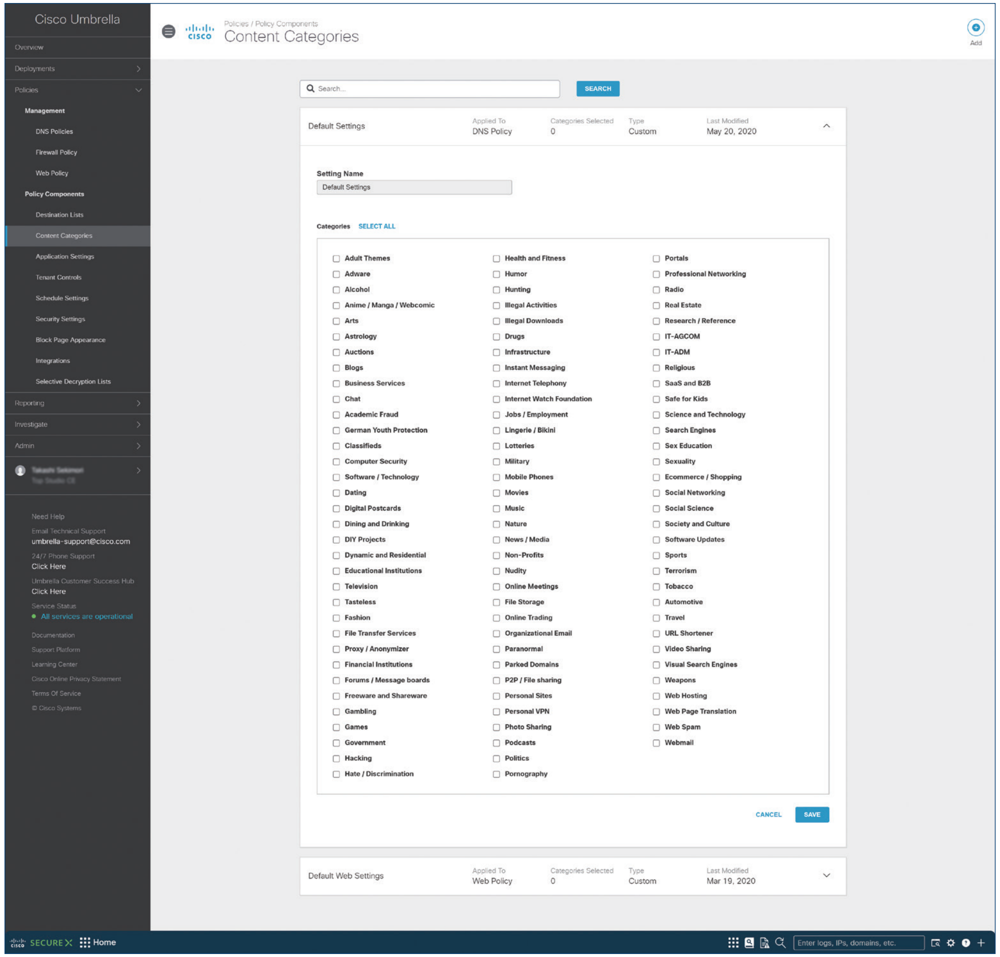


Roaming Devices
Windows/macOS (Umbrella Roaming Client)
Chromebook (Umbrella Chromebook Client)
iOS (Security Connector)

Manage Flexible, Location-aware Policies

Cisco Umbrella's 80+ content categories cover millions of domains (and billions of web pages) to give you control over which sites can be accessed by users on your network and by roaming users. The easy-to-use, cloud-delivered administration console enables you to quickly set up, manage, and test different acceptable use policies per network, group, user, device, or IP address, giving you greater control of your organization's internet usage. You even have the flexibility to set up different policies depending on whether users are on or off the corporate network.

Umbrella enables you to customize our category-based filtering to meet each network's unique needs to enable you to meet specific compliance requirements. Quickly create exceptions to allow or block specific domains, regardless of whether it is in a category that is allowed or blocked. Our 80+ content categories empower you to enforce acceptable web use to comply with internal policies or external regulations such as CIPA. We are also a member of the Internet Watch Foundation (IWF), enabling you to block their list of child sexual abuse sites.



Policies / Policy Components

Content Categories

	Applied To	Categories Selected	Type	Last Modified
Default Settings	DNS Policy	0	Custom	May 20, 2020

Setting Name: Default Settings

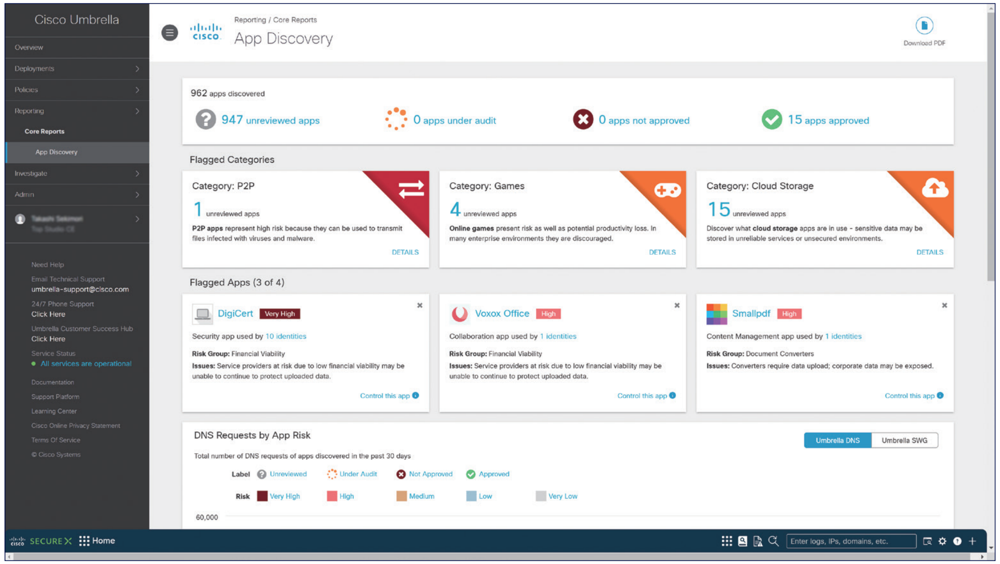
Categories SELECT ALL

□ Adult Themes
□ Adware
□ Alcohol
□ Anime / Manga / Webcomic
□ Arts
□ Astrology
□ Auctions
□ Blogs
□ Business Services
□ Chat
□ Academic Fraud
□ German Youth Protection
□ Classifieds
□ Computer Security
□ Software / Technology
□ Dating
□ Digital Postcards
□ Dining and Drinking
□ DIY Projects
□ Dynamic and Residential
□ Educational Institutions
□ Television
□ Tasteless
□ Fashion
□ File Transfer Services
□ Proxy / Anonymizer
□ Financial Institutions
□ Forums / Message boards
□ Freeware and Shareware
□ Gambling
□ Games
□ Government
□ Hacking
□ Hate / Discrimination
□ Health and Fitness
□ Humor
□ Hunting
□ Illegal Activities
□ Illegal Downloads
□ Drugs
□ Infrastructure
□ Instant Messaging
□ Internet Telephony
□ Internet Watch Foundation
□ Jobs / Employment
□ Lingerie / Bikini
□ Lotteries
□ Military
□ Mobile Phones
□ Movies
□ Music
□ Nature
□ News / Media
□ Non-Profits
□ Nudity
□ Online Meetings
□ File Storage
□ Online Trading
□ Organizational Email
□ Paranormal
□ Parked Domains
□ P2P / File sharing
□ Personal Sites
□ Personal VPN
□ Photo Sharing
□ Podcasts
□ Politics
□ Pornography
□ Portals
□ Professional Networking
□ Radio
□ Real Estate
□ Research / Reference
□ IT-AGCOM
□ IT-ADM
□ Religious
□ SaaS and B2B
□ Safe for Kids
□ Science and Technology
□ Search Engines
□ Sex Education
□ Sexuality
□ Ecommerce / Shopping
□ Social Networking
□ Social Science
□ Society and Culture
□ Software Updates
□ Sports
□ Terrorism
□ Tobacco
□ Automotive
□ Travel
□ URL Shortener
□ Video Sharing
□ Visual Search Engines
□ Weapons
□ Web Hosting
□ Web Page Translation
□ Web Spam
□ Webmail

	Applied To	Categories Selected	Type	Last Modified
Default Web Settings	Web Policy	0	Custom	Mar 19, 2020

Expose Shadow IT and Manage Cloud Adoption

Cloud usage is continuing to expand as end-users and departments become more comfortable acquiring cloud services. The typical organization is only aware of a small fraction of its overall cloud activity. The lack of a coordinated cloud enablement strategy leads to a broad set of productivity, expense, security, and support issues.



Reporting / Core Reports

App Discovery

962 apps discovered

947 unreviewed apps | 0 apps under audit | 0 apps not approved | 15 apps approved

Flagged Categories

Category: P2P
1 unreviewed apps
P2P apps represent high risk because they can be used to transmit files infected with viruses and malware.

Category: Games
4 unreviewed apps
Online games present risk as well as potential productivity loss. In many enterprise environments they are discouraged.

Category: Cloud Storage
15 unreviewed apps
Discover what **cloud storage** apps are in use - sensitive data may be stored in unreliable services or unsecured environments.

Flagged Apps (3 of 4)

DigiCert Very High
Security app used by 10 identities
Risk Group: Financial Viability
Issues: Service providers at risk due to low financial viability may be unable to continue to protect uploaded data.

Voxox Office High
Collaboration app used by 1 identities
Risk Group: Financial Viability
Issues: Service providers at risk due to low financial viability may be unable to continue to protect uploaded data.

Smallpdf High
Content Management app used by 1 identities
Risk Group: Document Converters
Issues: Converters require data upload; corporate data may be exposed.

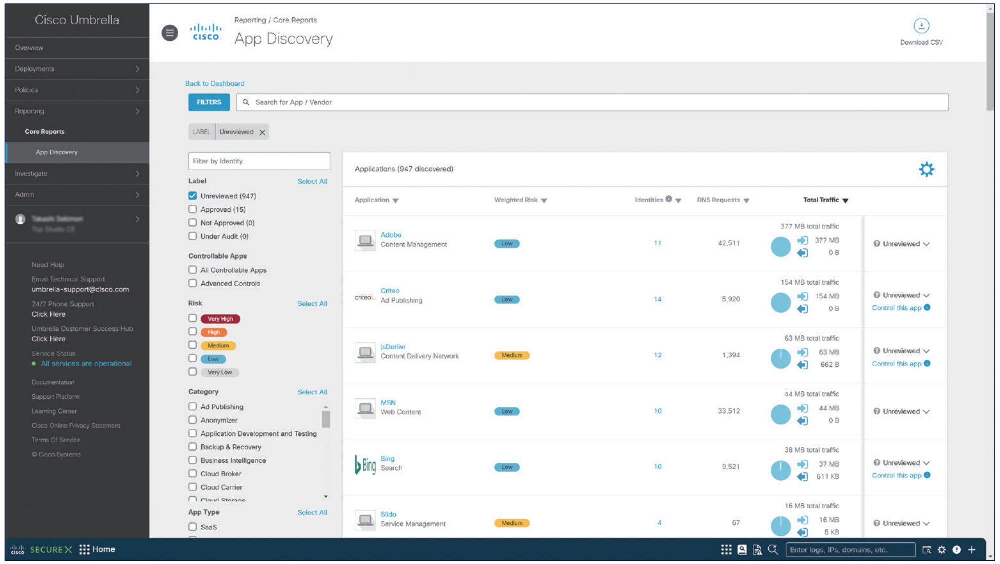
DNS Requests by App Risk

Total number of DNS requests of apps discovered in the past 30 days

Label: Unreviewed, Under Audit, Not Approved, Approved
Risk: Very High, High, Medium, Low, Very Low

The App Discovery dashboard provides an overview of the number of app requests by date and risk level to show patterns and changes over time. The most recent set of discovered and unreviewed apps are highlighted for easy access and a chart showing the number of apps in each major category is provided with a breakdown by risk level. These summary charts allow point and click access to more detailed information on the category or individual application to simplify common administrator tasks.

The App Discovery report included in Cisco Umbrella provides full visibility and risk information to manage cloud adoption in a secure and organized fashion. Once decisions are made about specific apps, you can block access to applications that are not approved to reduce the risk of sensitive data loss, account compromise, and malware infection.



Reporting / Core Reports

App Discovery

LABEL Unreviewed ×

Label
☑ Unreviewed (947)
☐ Approved (15)
☐ Not Approved (0)
☐ Under Audit (0)

Controllable Apps
☐ All Controllable Apps
☐ Advanced Controls

Risk
☐ Very High
☐ High
☐ Medium
☐ Low
☐ Very Low

Category
☐ Ad Publishing
☐ Anonymizer
☐ Application Development and Testing
☐ Backup & Recovery
☐ Business Intelligence
☐ Cloud Broker
☐ Cloud Carrier
☐ Cloud Storage

App Type
☐ SaaS

Applications (947 discovered)

Application	Weighted Risk	Identities	DNS Requests	Total Traffic	
Adobe Content Management	Low	11	42,511	377 MB total traffic 377 MB 0 B	Unreviewed
Criteo Ad Publishing	Low	14	5,920	154 MB total traffic 154 MB 0 B	Unreviewed Control this app
jsDerlivr Content Delivery Network	Medium	12	1,394	63 MB total traffic 63 MB 662 B	Unreviewed Control this app
MSN Web Content	Low	10	33,512	44 MB total traffic 44 MB 0 B	Unreviewed
Bing Search	Low	10	9,521	38 MB total traffic 37 MB 611 KB	Unreviewed Control this app
Slido Service Management	Medium	4	67	16 MB total traffic 16 MB 5 KB	Unreviewed

The Apps Grid report provides key details on all applications that have been discovered, including the app and vendor name, category, weighted risk level, number of users, number of requests, and current status. This report can be segmented and filtered into groups for deeper analysis by category, risk level, or number of users to provide views that assist with the organization and management of cloud adoption.

Simple and Effective Protection for Corporate and Guest Wi-Fi

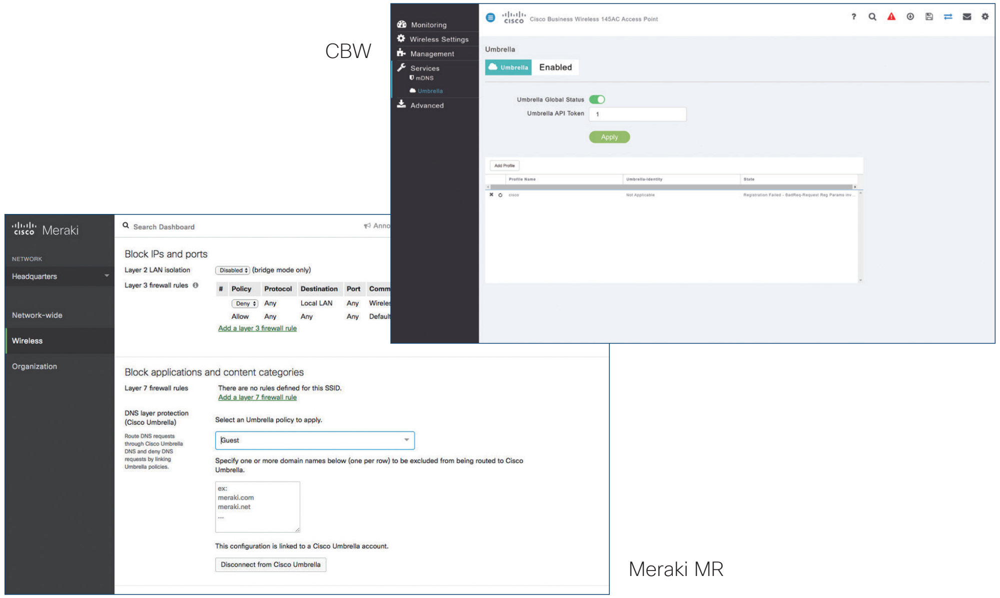
The Cisco Umbrella Wireless LAN (WLAN) package provides the first line of defense against threats for Wi-Fi connections. It offers the simplest, fastest way to protect every user on your Wi-Fi network.

Umbrella WLAN protects employees and guests who are accessing the internet from wireless access points. By enforcing security at the DNS layer, connections to unsafe sites are never established and malicious files are never downloaded. This prevents malware from infecting devices and stops attacks from exfiltrating data over any port and protocol. Umbrella WLAN also brings a simple-to-use content filtering solution to your Wi-Fi network. It stops guests and corporate users from accessing inappropriate content, based on company policy. This keeps users happy with safe internet access, while also protecting your business.

Umbrella WLAN is the simplest way to protect any device accessing your wireless network — there's no action required from end-users for protection. Whether it's a corporate device, employee-owned, or customer-owned device, Umbrella WLAN adds an easy, but very effective layer of protection.

Umbrella WLAN works across a broad portfolio of wireless controllers and access points. Built-in integrations with the Cisco Business Wireless Access Points (CBW), Cisco Embedded Wireless Controller (EWC) on Catalyst 9100 Access Points, Cisco Wireless Controllers, and Cisco Meraki MR Cloud Managed Access Points provides additional ease of use and granularity.

CBW



Cisco Business Wireless 145AC Access Point

Monitoring
Wireless Settings
Management
Services
mDNS
Umbrella
Advanced

Umbrella

Umbrella Enabled

Umbrella Global Status: ●
Umbrella API Token: 1

Apply

Add Profile

	Profile Name	Umbrella-Identity	State
✖ ○	cisco	Not Applicable	Registration Failed - BadReq-Request Reg Params inv...

cisco Meraki

Search Dashboard

NETWORK
Headquarters
Network-wide
Wireless
Organization

Block IPs and ports

Layer 2 LAN isolation: Disabled (bridge mode only)

Layer 3 firewall rules

#	Policy	Protocol	Destination	Port	Comm
	Deny	Any	Local LAN	Any	Wireles
	Allow	Any	Any	Any	Default

Add a layer 3 firewall rule

Block applications and content categories

Layer 7 firewall rules: There are no rules defined for this SSID.
Add a layer 7 firewall rule

DNS layer protection (Cisco Umbrella)

Route DNS requests through Cisco Umbrella DNS and deny DNS requests by linking Umbrella policies.

Select an Umbrella policy to apply.

Guest

Specify one or more domain names below (one per row) to be excluded from being routed to Cisco Umbrella.

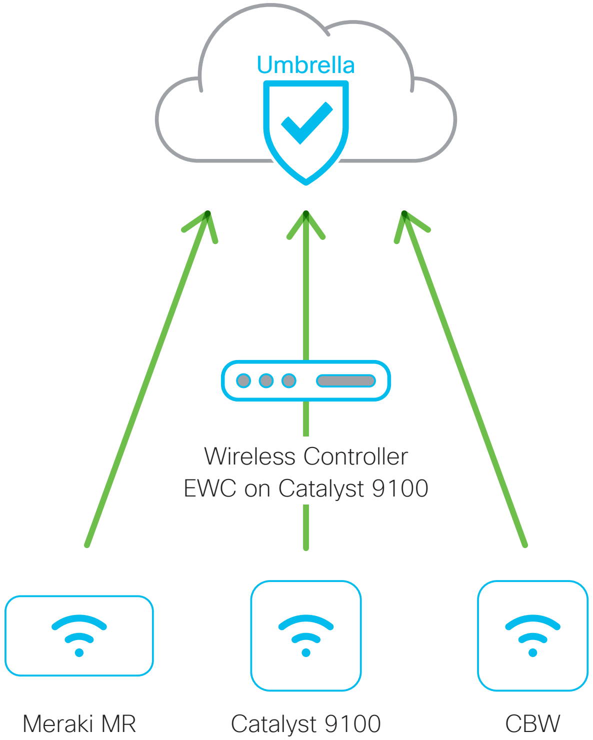
ex:
meraki.com
meraki.net
...

This configuration is linked to a Cisco Umbrella account.

Disconnect from Cisco Umbrella

Meraki MR

You can deploy Umbrella in minutes across your access points.
Simply input the API key and secret from Umbrella into the AP's GUI.

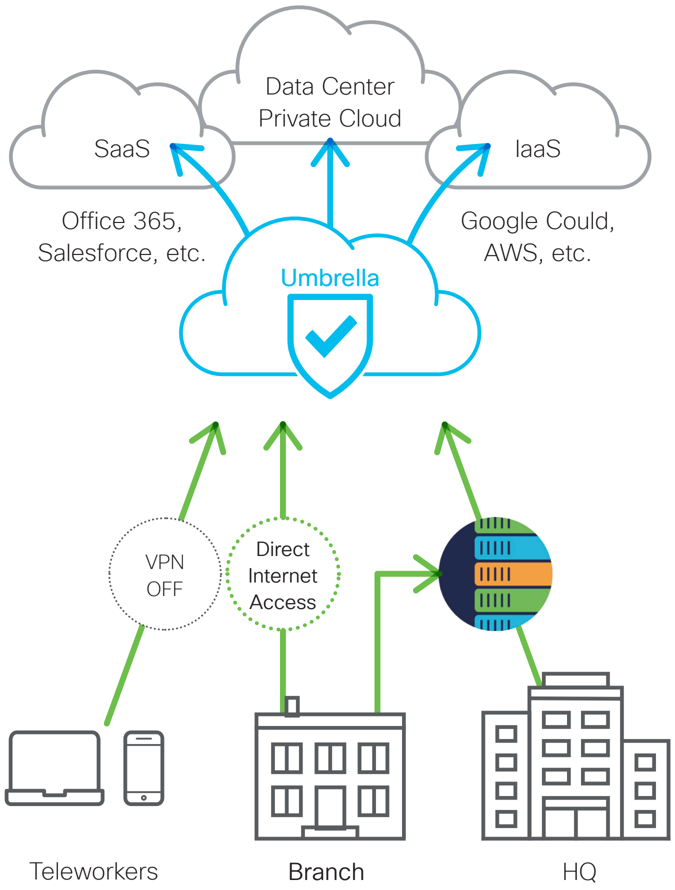


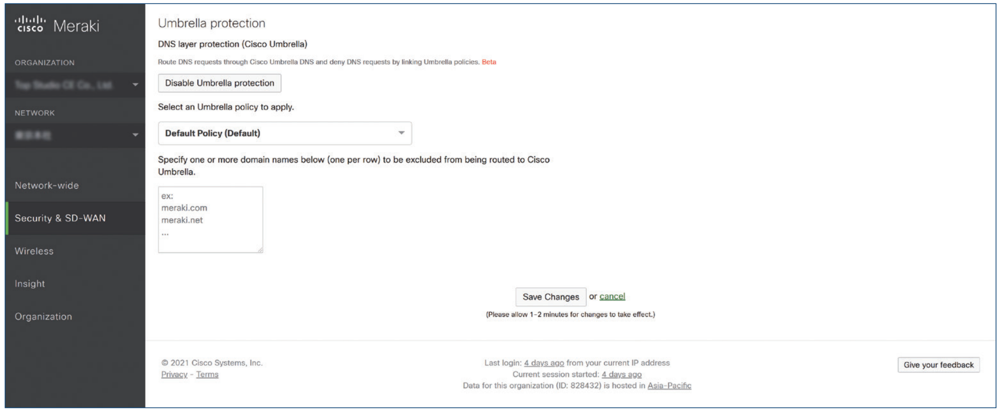
The Simplest Way to Provide DNS Security for Direct Internet Access (DIA) from Branch Offices from Branch

The traditional WAN was built to give branch offices and roaming users access to IT resources within private data centers. But today, as networks become more decentralized and users connect directly to SaaS applications, backhauling traffic to apply security policies just isn't efficient. And that's not the only problem. Backhauling internet-bound traffic is expensive, and it adds latency. So users get frustrated — and thwarted — in their attempt to get work done. That's why so many branch offices are migrating to DIA.

The Cisco Umbrella integration enables a cloud-based security service by inspecting the Domain Name System (DNS) query that is sent to the enterprise DNS server through the Cisco RV Series, Cisco Meraki MX Cloud Managed Security & SD-WAN Appliances, Cisco ISR 1000 Series, Cisco ISR 4000 Series, and Cisco Catalyst 8000 Series Edge Platforms. It provides the first layer of defense against threats at branch offices. And it offers the simplest, fastest way to protect every device on your branch network. You gain visibility and enforcement at the DNS-layer, so you can block requests to malicious domains and IPs before a connection is ever made.

Cisco Umbrella protects employees and guests in distributed branch offices — like those in retail, finance, hospitality, and education. By enforcing security at the DNS-layer, connections are never established and files are never downloaded. This prevents malware from infecting devices and stops attacks from exfiltrating data over any port.





[redacted]

[redacted]

Umbrella protection

DNS layer protection (Cisco Umbrella)

Route DNS requests through Cisco Umbrella DNS and deny DNS requests by linking Umbrella policies. Beta

Select an Umbrella policy to apply.

Default Policy (Default)

Specify one or more domain names below (one per row) to be excluded from being routed to Cisco Umbrella.

ex:
meraki.com
meraki.net
...

(Please allow 1-2 minutes for changes to take effect.)

© 2021 Cisco Systems, Inc.
Privacy - Terms

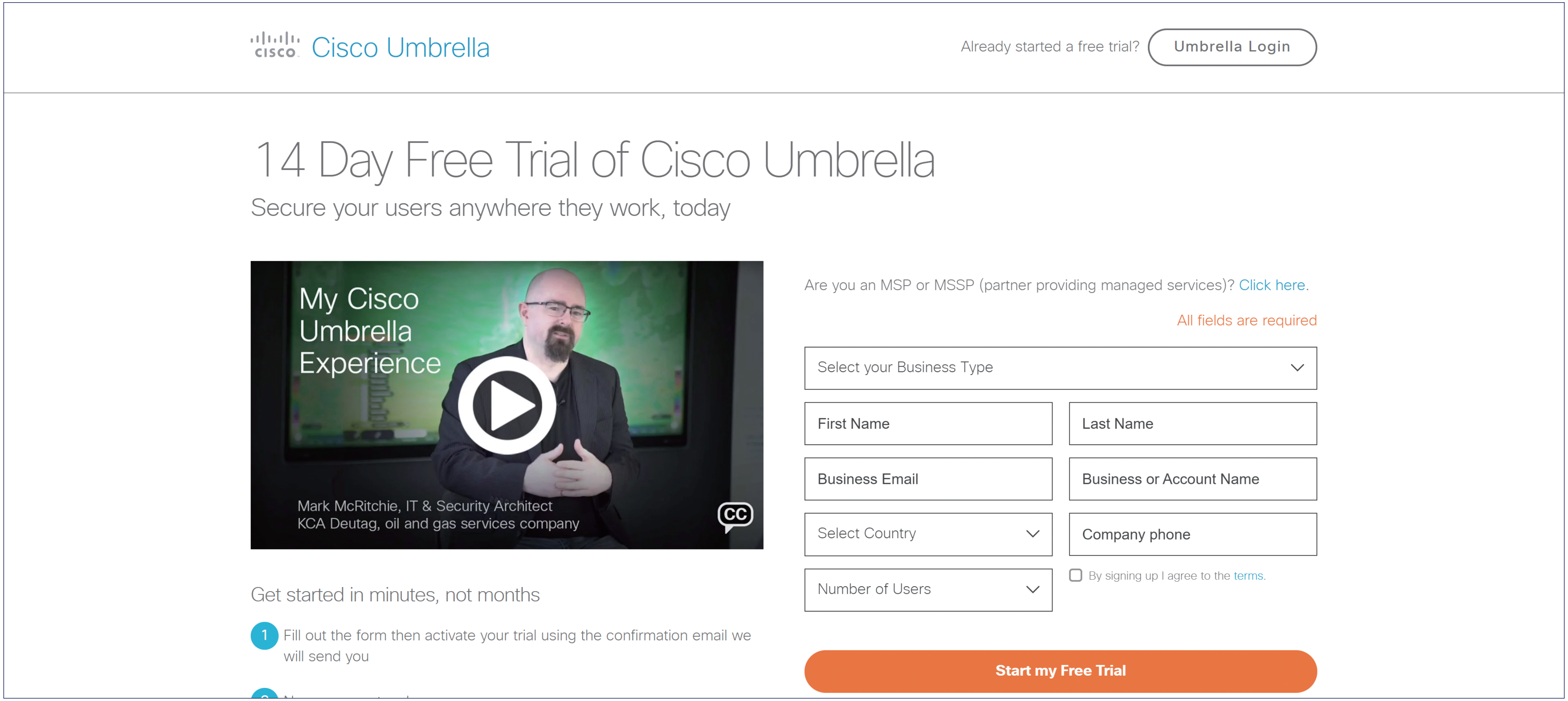
Last login: 4 days ago from your current IP address
Current session started: 4 days ago
Data for this organization (ID: 828432) is hosted in Asia-Pacific

You can deploy Umbrella in minutes on your Meraki MX.
Simply input the API key and secret from Umbrella into Meraki dashboard.

Free Umbrella 14-Day Trial

If you want to add an additional layer of DNS security to your router or firewall, try our free trial. You can set it up yourself in less than five minutes, no credit card or phone call required.

WEB signup.umbrella.com



Cisco Umbrella
Already started a free trial?
Umbrella Login

14 Day Free Trial of Cisco Umbrella

Secure your users anywhere they work, today

My Cisco Umbrella Experience
Mark McRitchie, IT & Security Architect
KCA Deutag, oil and gas services company
CC

Are you an MSP or MSSP (partner providing managed services)? Click here.

All fields are required

Select your Business Type

First Name

Last Name

Business Email

Business or Account Name

Select Country

Company phone

Number of Users

□ By signing up I agree to the terms.

Start my Free Trial

Get started in minutes, not months

1 Fill out the form then activate your trial using the confirmation email we will send you